IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA,	)	
	)	8:13CR105
Plaintiff,	)	
	)	
v.	)	
	)	
TIMOTHY DEFOGGI,	)	
	)	
Defendant.	)	

OPPOSITION BRIEF OF THE UNITED STATES IN RESPONSE TO DEFENDANT'S MOTION TO SUPPRESS EVIDENCE OBTAINED THROUGH SEARCH OF DEFENDANT'S HOUSE

Prepared and Submitted by:

DEBORAH R. GILG
United States Attorney
for the District of Nebraska

MICHAEL P. NORRIS (#17765)
Assistant U.S. Attorney
1620 Dodge Street, Suite 1400
Omaha, Nebraska 68102-1506
Phone: (402) 661-3700

KEITH BECKER
DOJ Trial Attorney
1400 New York Ave NW 6th Floor
Washington, DC 20530
Phone: (202) 305-4104

SARAH CHANG
DOJ Trial Attorney
1400 New York Ave NW 6th Floor
Washington, DC 20530
Phone: (202) 353-4979

Defendant Timothy DeFoggi (hereinafter DeFoggi) has filed a motion to suppress evidence obtained from a search of defendant's residence, Dkt. Nos. 105-107, to which the government hereby responds in opposition. Through this motion, DeFoggi seeks to suppress evidence derived from the execution of a search warrant authorizing a search of his residence that was authorized by a neutral magistrate upon a finding of probable cause. For the reasons discussed herein, the Court should deny the defendant's motion.

I. FACTS

On March 20, 2013, a Grand Jury sitting in the District of Nebraska returned a seven-count Indictment against defendant DeFoggi along with a co-conspirator. Count I of the Indictment charges DeFoggi with engaging in a child exploitation enterprise, in violation of 18 U.S.C. § 2252A(g). Count II of the Indictment charges DeFoggi with conspiracy to advertise child pornography, in violation of 18 U.S.C. § 2251(d)(1) and (e). Count III of the Indictment charges DeFoggi with conspiracy to distribute child pornography, in violation of 18 U.S.C. § 2252A(a)(2) and (b)(1). Counts IV-VII of the Indictment charges DeFoggi with accessing with intent to view child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B). The charges relate to DeFoggi's activity on or about March 2, 2012 through December 8, 2012 on a child pornography website described as "Website A."

A. "Website A"

As alleged in the Indictment, "Website A," whose name is known to the Grand Jury, was a child pornography social networking website whose primary purpose was the advertisement and distribution of child pornography and the discussion of matters pertinent to the sexual abuse of children. "Website A" operated from March of 2012 until December of 2012. On November 18, 2012, the computer server hosting "Website A" was seized from a web-hosting facility in Bellevue, Nebraska. The website remained operating in Omaha, Nebraska, from November 19,

2012, until December 8, 2012, at which time "Website A" ceased to operate. Between November 19, 2012, and December 8, 2012, law enforcement agents acting pursuant to an order of the United States District Court for the District of Nebraska monitored electronic communications of users of "Website A." Before and after its seizure by law enforcement, law enforcement agents viewed, examined and documented the contents of "Website A," which are described below.

The name of "Website A" contained a term referring to a sexual interest in children. As of December 8, 2012, the site listed over 8,100 members. The rules of the site, which were accessible on the main page to anyone who accessed "Website A," described it as a tool for communication among pedophiles to discuss their interests and share "content" – content referring to child pornography.

Users could register on "Website A" with a username and a password. Once registered, users could set up a profile that included a picture, personal information, contact information, and other functions such as blogs, uploaded files, web pages, or polls. Many users had a user photo, sometimes called an "avatar," that was in and of itself an image of child pornography. Although users could register and set up their own profiles, registration was not required to access "Website A." Any user could access most of the site, including postings of child pornography, anonymously without registering or logging in.

"Website A" contained a section that compiled all files posted by members. Within that section were images and videos. The section contained more than 17,000 images, all of which depicted children. All of those images were accessible to any user who accessed the site, whether registered or not. Those images depicted minor children engaging in sexually explicit conduct with adults or other children, minor children posed while exposing their genitals, or images of child erotica. Most of those images were of prepubescent children. Many of those images depicted infant and toddler-aged children being sexually abused by adults or posed to expose their

genitals. The section also contained approximately 120 videos. Videos posted included videos of minor children, some of whom are prepubescent, engaging in sexually explicit conduct with adults or other children.

"Website A" also contained a section for members to set up groups. There were over 300 groups on "Website A." Any member could start a group. Within a group, members could post images and messages which were visible to all group members. Groups could be open or closed. The vast majority of groups on "Website A" were open. In an open group, all users who accessed the board, even those who had not registered and logged in with a username and password, could view images and messages posted to the group. In a closed group, messages and images were visible only to group members.

The names and descriptions of all groups on "Website A" were listed and visible to anyone who accessed the site, whether the group was open or closed. The number of members in any given group varied from a handful to dozens to hundreds to over a thousand. Open groups which were accessible to all users essentially functioned as labels or subcategories for postings of distinct types of child pornography on the site. For example, there was a group with over 1,000 members whose group description stated it was for pictures and videos produced only in 2012. That group contained numerous images of infant and toddler aged children whose genitals are exposed and/or are being subjected to sexual abuse. Other open groups on "Website A" were dedicated to, for example: sexually explicit images of kindergarten age girls ages 4-8 and images of infant and toddler aged children being sodomized. Other open groups with more than 100 members included groups dedicated to incest, female pedophiles, boy pedophiles, pedophilic videos with "no limits" – which refers to violent sexual activity; and videos of infant children. Within those groups, the group descriptions and images posted within them were consistent with their group

titles. All of those groups contained images of minor children engaging in sexually explicit conduct with adults or other children, or posed to expose their genitals.

"Website A" users utilized advanced technological means in order to undermine law enforcement's attempts to identify them. For example, "Website A" was technically designed to facilitate anonymous communication by its users, whether they were registered or not. Only a user who had installed special software on the user's computer could access "Website A." That software enabled the communications of "Website A" users to be routed through multiple computers in order prevent communications from being traced back to the users.

"Website A" users also frequently discussed and advised each other about security, anonymity, and preventing detection by law enforcement. For example, multiple users posted entries in "Website A" "blogs" available to all "Website A" users about: the proper use of encryption software and techniques to hide and/or password-protect child pornography collections in the event of a law-enforcement search; programs to be used to wipe or "clean" data from a user's computer; and software that could be used to browse the Internet and download child pornography in such a way as to maintain the user's anonymity online. In addition, a group existed whose description stated that it was dedicated to discussing how to identify other actual pedophiles in the real world and online, and how to distinguish someone claiming to have actual access to a child from someone who might be a law enforcement agent.

II. ARGUMENT

A. The Defendant's Motion to Suppress (Dkt. Nos. 105-107)

The defendant's motion to suppress seeks to suppress evidence seized from the defendant's residence during the April 9, 2013 search on the theory that the affidavit submitted in support of the residential search warrant lacked sufficient probable cause.

1. The Residential Search Warrant Articulated Probable Cause for

the Search

The defendant claims that the affidavit in support of the search of his residence did not establish probable cause. Dkt. No.1-6 at pp. 2-5. "An affidavit establishes probable cause for a warrant if it sets forth sufficient facts to establish 'a fair probability that contraband or evidence of a crime will be found in a particular place." United States v. Darr, 661 F.3d 375, 380 (8th Cir. 2011) (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983)). A determination of whether probable cause exists "requires a commonsense analysis of the facts available to the judicial officer who issued the warrant." United States v. Colbert, 605 F.3d 573, 576 (8th Cir. 2010) (citing Gates, 462 U.S. at 230, 238). Further, the determination of the issuing magistrate is due "great deference by reviewing courts." Gates, 462 U.S. 236; see also United States v. McArthur, 573 F.3d. 608, 613 (8th Cir. 2009).

There was probable cause to believe that there would be evidence of a crime at the defendant's residence. The affidavit in support of the warrant detailed a methodical investigation by law enforcement which determined that the defendant accessed a website containing child pornography. That warrant, warrant application and affidavit are attached as Exhibit 1. It described in great detail what "Website A" was and how it worked, specified particular sections of "Website A" that the defendant accessed, and described particular images of child pornography on "Website A" the defendant accessed. The affidavit then demonstrated, in exhaustive detail, how investigators linked defendant to activity conducted on "Website A."

The affidavit summarized that according to data obtained from logs on "Website A," and monitoring by law enforcement, a user account was created on or about April 18, 2012, with the username "fuckchrist" and display name "PTasseater."[1] That account remained active until "Website A" ceased to operate on December 8, 2012. According to law enforcement review of

1 A username or login name is entered along with a password when the user logs into the site. A display name is a name that appears on the site when a user takes an action on the site, such as posting a message.

"Website A" activity, username "fuckchrist" was a member of multiple groups through which "fuckchrist" had accessed numerous child pornography images. Law enforcement also reviewed private messages sent by "PTasseater"/"fuckchrist" to other "Website A" users and found that dozens of those private messages advocated and described an interest in the violent rape of children, including infant and toddler-aged children, in graphic language and detail. Multiple private messages also described his location as in or near "DC."

The affidavit then stated that during the course of law enforcement's investigation into "Website A," an FBI online covert employee (OCE) contacted "PTasseater"/"fuckchrist" via the private messaging feature provided by "Website A." In the course of this contact, "PTasseater"/"fuckchrist" provided the FBI OCE with the electronic mail (e-mail) address fuckchrist@tormail.org and indicated an interest in the murder of "little ones" and violent child exploitation material. "PTasseater" / "fuckchrist" also stated that he normally accessed the Network on which "Website A" operated between 4:00am and 6:00am Eastern time ("early in the morning") and again between 4:30pm and 6:00pm Eastern time.

According to the affiant, username "ptasseater" was also located on an image hosting website known to be used for the upload and distribution of child exploitation images. A review of information available to law enforcement from this website indicated the account was created on or about July 7, 2007, and associated with e-mail addresses jsnparsons@yahoo.com and ptasseater@gmail.com. As of March 28, 2013, the current status for this account showed as locked due to indecent comments.

The "ptasseater" account on the image hosting website bore numerous similarities to the "PTasseater"/"fuckchrist" account on "Website A." For instance, the profile of the "ptasseater" account on the image hosting website stated:

> "Love fantasy chat and comments. To the lawless Governments who try and criminalize consentual sex, you need to reject Christianity. Christ's father was a

> pedophile. He was in his 80's and Mary 12 when they were married. Christ had 4 brothers through sex. That makes Joseph a "sexual predator". You can't be a Christian and condemn adult/youth relationships. Like it or not, that's history."

Information available to law enforcement from the image hosting website showed that user "ptasseater" made dozens of comments about images posted on the site. Most of the comments were sexual in nature and many of those comments advocated the violent rape and in some cases murder of the persons depicted in the pictures about which "ptasseater" was commenting, of a highly similar nature and tone to the comments frequently made by "PTasseater"/"fuckchrist" on "Website A." Although not all of the images about which "ptasseater" commented remain available for review by law enforcement, the text of the comments made it evident that many of the pictures about which "ptasseater" was commenting depicted children. The affidavit stated that a review of those images that remain available from the image hosting website demonstrated that the images predominantly depicted underage males and females, however, none of the images still available depicted child pornography.

The affidavit then discusses in detail, how a review of IP addresses associated with the account "ptasseater" on the image hosting website showed that between May 27, 2011, and December 18, 2011, the account "ptasseater" conducted its activities, numbering more than 400, from IP address 96.231.186.155, which resolved to Verizon Internet Services. In response to legal process, Verizon Internet Services provided the following subscriber information associated with IP address 96.231.186.155:

> Session Details for IP Address 96.231.186.155
> Assigned Start: May 13, 2011 19:48pm Z
> Update Time: May 23, 2012 01:51am Z
> Customer Name: Tim DeFoggi
> Account Address: 20311 Crown Ridge Court, Germantown, Maryland 20874
> Daytime Telephone Number: (703) 909-5559
> E-Mail Address: deparmentofstate@yahoo.com
> Account Number: 0118336397875
> User ID: vze17v3h6

That information indicates that Tim DeFoggi was assigned IP address of 96.231.186.155 between May 13, 2011, and May 23, 2012 – inclusive of the time in which "ptasseater" accessed the image hosting site over 400 times from that IP address.

The affidavit also provided information obtained from a subject under investigation by the FBI for activities related to child exploitation material concerning the activity of an individual initially identified as "Jeff," a member of "boylover.net," a known website for underage male child exploitation material, who utilized e-mail addresses ptasseater@hotmail.com, notaboo_69@yahoo.com, luvemskinny@yahoo.com, and cellular telephone number (703) 909-5559. This individual provided investigators with another individual who had personally met "Jeff." This second individual was interviewed in October 2006 and stated that "Jeff" provided him a true name of "Tim" and that "Jeff"/"Tim" held a government security clearance and worked in the Washington, DC, area.

The affidavit then linked the telephone number associated with "Jeff"/"Tim" as well as "ptasseater" with defendant, by discussing information provided by Cingular Wireless related to cellular telephone number (703) 909-5559:

> Account Number: 923887518
> Account Holder: Timothy DeFoggi
> Date of Birth (DOB): January 8, 1958
> Social Security Account Number (SSAN): ***-**-****
> Credit Address: 8760 Mill Towns Court, Alexandria, VA 22309
> Home Phone: (703)555-6969
> Home E-Mail: mct_cni@hotmail.com
> Active:06/17/2003
> Photo ID: Florida Driver's License D120816580080

Next, the affidavit laid out all the open source information checks that led investigators back to defendant. For example, a check of open source information from the Internet regarding "PTasseater" revealed a profile on the website dickflash.com associated with the username "showgenitals." An America Online (AOL) Instant Messenger (AIM) username "ptasseater" was

associated with this dickflash.com profile along with e-mail address genericaddr@yahoo.com. In response to legal process, AOL provided the following information related to AIM username "ptasseater":

> ZIP: 90210
> Screen Names: luvemskinny@yahoo.com
> Since (Membership): September 11, 2003
> IP logs were provided from August 8, 2012 through November 21, 2012

The luvemskinny@yahoo.com address was significant in that it was associated with telephone number (703) 909-5559, used by "Jeff"/ "Tim" and subscribed to by defendant. The affidavit also details how investigators, using the IP logs provided by AOL, found that the IP addresses from which activity was being conducted by AIM username "ptasseater" resolved back to the following subscriber:

> Session Details IP address 173.73.10.249
> Start Time: October 30, 2012, 17:49pm UTC
> Stop Time: In use on the date of legal process
> Session Details IP address 71.178.217.239
> Start Time: June 30, 2012, 08:22am UTC
> Stop Time: October 30, 2012, 01:37am UTC
> Customer Name: Tim DeFoggi
> Account Address: 20311 Crown Ridge Court, Germantown, Maryland 20874
> Daytime Telephone Number: (703)909-5559
> E-Mail Address: deparmentofstate@yahoo.com
> Account Number: 0118336397875
> User ID: vze17v3h6

The affidavit also summarizes additional checks conducted related to e-mail address ptasseater@gmail.com which identified subscriber profile 399710447 on myspace.com (subscriber profile address: myspace.com/399710447). In response to legal process, myspace.com provided the following information related to subscriber profile 399710447:

> First/Last Name: Jack Hoff
> E-mail address: ptasseater@gmail.com
> Sign up IP/Date: 98.169.184.202; July 26, 2008, 03:14am

Defendant claims that the myspace.com page associated with subscriber number

399710447 now shows an individual other than the defendant and summarily concludes that this brings into question all other investigative discoveries linking defendant to "Website A." Dkt. No. 106, p. 5. Defendant's claim ignores all other possibilities. For example, it is possible that myspace.com deletes inactive profiles and reassigns them. It is also possible that someone with access to defendant's myspace.com page changed the profile picture and name associated with the page. Even if the defendant is correct in his claim that the government misidentifies this particular myspace.com page as belonging to the defendant, it is one small and relatively inconsequential piece of an extensive probable cause showing demonstrated by the affidavit.

The affidavit then further compares the different accounts from open sources on the Internet and responses from legal process connected to the username "PTasseater" to reveal that the same IP address was utilized for three separate e-mail addresses on four separate occasions. A review of registration and login information related to IP address 72.196.200.230 showed the following:

i. notaboo_69@yahoo.com Last Login August 22, 2006; 11:58am EDT

ii. luvemskinny@yahoo.com Registration September 16, 2006, 16:57 GMT

iii. luvemskinny@yahoo.com Last Login October 24, 2006; 00:17am GMT

iv. jsnparsons@yahoo.com Account Creation April 27, 2007, 23:27pm GMT

In addition, a review of IP logs associated with the username "PTasseater" from the image hosting website detailed above revealed two IP addresses that accessed both the image hosting site as well as a Google e-mail account and the Myspace.com account also associated with username "PTasseater":

b. IP Address 68.106.107.49

i. Google (ptasseater@gmail.com registration): February 3, 2008

ii. Image Hosting Website: July 8, 2007 to April 21, 2008

c. IP Address 98.169.184.202

i. Myspace Registration: July 26, 2008

ii. Image Hosting Website: July 10, 2008 to August 24, 2008

And lastly, the affidavit discusses results from a pen register / trap trace (PRTT) obtained for the Verizon Internet Service account associated with 20311 Crown Ridge Court, Germantown, Maryland. A review of the PRTT information collected between January 12, 2012, and January 26, 2012, showed Internet connections to IP addresses associated with the Network primarily in the early morning or late evening hours, consistent with statements made by "PTasseater" / "fuckchrist" concerning use of the Network as detailed above.

According to the affidavit, open source database checks confirmed that Timothy Ray DeFoggi, DOB: January 8, 1958, SSAN: 263-35-0241 currently resides at 20311 Crown Ridge Court, Germantown, Maryland 20874.

On or about March 27, 2012, investigators received information from the United States Postal Service's (USPS) Delivery Unit that services 20311 Crown Ridge Court, Germantown, Maryland 20874. USPS personnel indicated that an individual utilizing the name Timothy R. Defoggi is currently receiving mail at that residence.

On or about March 27, 2012, a vehicle with Maryland license plate 5AJ8476 was observed at the aforementioned residence. A check with the Department of Motor Vehicles showed that this vehicle is registered to Timothy R. Defoggi at the 20311 Crown Ridge Court.

In sum, the affidavit in support of the search warrant executed at the defendant's residence spelled out in great detail the criminal activity that led to the issuance of the warrant. The warrant thoroughly described "Website A," how it operated, and the quality and quantity of child pornography content that was available on it. Ex. 1, S. Warr. Aff. at ¶¶ 9-17. It detailed the network that "Website A" operated on and the affirmative steps users needed to take in order to

access "Website A." Id. at ¶¶ 18-19. The affidavit also thoroughly described in great detail the child pornography accessed by the IP address ultimately tied to the defendant. In particular, it described that according to data obtained from logs on "Website A" and monitoring by law enforcement, on November 22, 2012, while a member of the "Website A" group known as "Anything Goes – Hardcore Child Fucking," a user with the associated screen names "PTasseater"/"fuckchrist" accessed an image which depicted a prepubescent minor female and an adult male facing each other. The adult male can be seen with his hand placed on the minor female's head while the minor performs oral sex on him. Ex. 1, S. Warr. Aff. at ¶ 20a. The affidavit articulated detailed descriptions of two more child pornography images accessed by user "PTasseater"/"fuckchrist." Id. at ¶ 20b-20c.

The affidavit next details the further investigation that led to the search of the defendant's home. In particular, it set forth how analysis of data gathered through the image hosting website, open source information, and subsequent follow up via administrative subpoenas revealed that the individual utilizing the screenname/login "PTasseater" / "fuckchrist" on "Website A" is an individual residing at defendant's home address. Ex. 1, S. Warr. Aff. at ¶¶ 23-47. The affidavit also articulated characteristics common to individuals who conspire to advertise, distribute, and view child pornography and reasons why the user under investigation was likely to display those characteristics, Id. at ¶¶ 48-49, and requested to enter the home without announcing and to place the affidavit under seal. Ex. 1, at pp. 15, 36-37.

Defendant's access to child pornography images on "Website A" provides strong evidence that he possesses the material. See United States v. Wagers, 452 F.3d 534, 540 (6th Cir. 2006) (noting that "evidence that a person has visited or subscribed to websites containing child pornography supports the conclusion that he has likely downloaded, kept, and otherwise possessed the material."). Indeed, as the Eighth Circuit has noted,

> [t]he observation that images of child pornography are likely to be hoarded by persons interested in those materials in the privacy of their homes is supported by common sense and the cases. Since the materials are illegal to distribute and possess, initial collection is difficult. Having succeeded in obtaining images, collectors are unlikely to [ ] destroy them. Because of their illegality and the imprimatur of severe social stigma such images carry, collectors will want to secret them in secure places, like a private residence.

McArthur, 573 F.3d at 613-14 (quoting United States v. Riccardi, 405 F.3d 852, 861 (10th Cir. 2005)).

Moreover, the affiant opined based upon her training and experience and the specific facts of the investigation that the target of the investigation was likely to have collected child pornography materials in the target's home. A court is entitled to rely on an affiant's expertise regarding characteristics and tendency of child pornography consumers when determining whether there is sufficient probable cause to issue a warrant. United States v. Watzman, 486 F.3d 1004, 1008 (7th Cir. 2007) (explaining district court entitled to rely on affiant's expertise regarding tendency of child pornography consumers to "hoard collections at home" in concluding probable cause existed to search defendant's home).

The issuing magistrate therefore made a practical, common sense decision, that, given all of the circumstances set forth in the affidavit before him, there was a fair probability that contraband or evidence of a crime would be found at that particular place. The defendant's accessing of child pornography images on "Website A" supported the belief that there was probably evidence of his receipt and possession of child pornography on one or more computers at his residence.

The defendant claims that the affidavit does not establish sufficient probable cause to link him to activity conducted on "Website A" by user "PTasseater"/"fuckchrist." Dkt. No. 106 at pp. 2-5. Defendant's claim obfuscates the investigative steps and subsequent IP address analysis set forth in the search warrant affidavit. Contrary to defendant's assertions, there were more than three

connections linking defendant to activity on "Website A" conducted by "PTasseater"/"fuckchrist." See Dkt. No. 106, p. 3. As detailed above, not only did the image hosting website profile contain numerous similarities to the user "PTasseater"/"fuckchrist" on "Website A," i.e. expressing a specific interest in the violent rape of children, but the IP addresses associated with the image hosting website profile resolved to a Tim DeFoggi residing at 20311 Crown Ridge Court, Germantown, Maryland 20874 with a phone number of (703) 909-5559, which is the same address and person linked to the AIM username "ptasseater." Furthermore, interviews conducted with an individual under investigation for activities related to child exploitation material led investigators to a "Jeff," who was a member of a website used to share underage male child exploitation material, whose true name was "Tim" and lived in the Washington, DC area with a government security clearance. The user "PTasseater"/"fuckchrist" on "Website A" had discussed through private messages that he lived in the Washington, DC area and expressed a specific interest in the violent rape of children. The affidavit's establishment of probable cause did not rely wholly on matching the terms "PTasseater" and "fuckchrist" on "Website A" to same or similar usernames on other internet websites and service platforms. Rather, it was the combined effect of having found identical usernames across a spectrum of internet service platforms, in conjunction with source information, "Website A" activity, and IP address analysis that led investigators to conclude that there was fair probability that evidence of child exploitation material activity would be found at the defendant's residence.

In any event, "[f]inely-tuned standards such as proof beyond a reasonable doubt or by a preponderance of the evidence, useful in formal trials, have no place in the magistrate's decision . . . it is clear that only the probability, and not a prima facie showing, of criminal activity is the standard for probable cause." Gates, 462 U.S. at 235 (internal citations omitted). The affidavit need not have established proof beyond a reasonable doubt of that crime, merely a fair probability

that evidence or contraband will be found at the premises.

2. The Good-Faith Exception Applies

In any event, even assuming *arguendo* that probable cause was lacking in sufficiency, the Leon good faith exception would allow the admissibility of the evidence obtained from the residential search.

In United States v. Leon, 468 U.S. 897 (1984), the Supreme Court carved out an exception to the exclusionary rule by determining that evidence which would otherwise be inadmissible because the warrant was invalid would nonetheless be admissible if the evidence was obtained by law enforcement officers who were acting in reasonable good faith reliance upon the search warrant issued by a neutral and detached magistrate. The Supreme Court found that reliance on an invalid search warrant would not be reasonable if: (1) the affidavit included information the officer knew was false or would have known to be false except for the officer's reckless disregard for the truth and such information misled the issuing magistrate; (2) the issuing magistrate abandoned a neutral and detached role; (3) the warrant was based on an affidavit with so few indicia of probable cause that an objective belief in its validity would be unreasonable; and (4) the warrant itself was so facially deficient that the executing officers could not rely upon its validity. Leon, 468 U.S. at 923; see United States v. Perry, 531 F.3d 662, 665 (8th Cir. 2008). None of those exceptions apply in this case. Accordingly, the motion to suppress evidence derived from the residential search should be denied.

III. CONCLUSION

For the reasons stated above, the United States respectfully submits that the defendant's motions to suppress evidence be denied.

Respectfully submitted,

UNITED STATES OF AMERICA,
Plaintiff

DEBORAH R. GILG
United States Attorney

By: s/ Michael P. Norris
MICHAEL P. NORRIS (#17765)
Assistant United States Attorney
1620 Dodge Street, Suite 1400
Omaha, Nebraska 68102-1506
(402) 661-3700

s/Keith Becker
KEITH BECKER
DOJ Trial Attorney
1400 New York Ave NW 6th Floor
Washington, DC 20530
(202) 305-4104

s/Sarah Chang
SARAH CHANG
DOJ Trial Attorney
1400 New York Ave NW 6th Floor
Washington, DC 20530
(202) 353-4979

CERTIFICATE OF SERVICE

I hereby certify that on March 13, 2014, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which sent notification of such filing to the following: John S. Berry, Attorney at Law at john@jsberrylaw.com.

s/Sarah Chang
SARAH CHANG
Trial Attorney